УДК 351.862.48
DOI 10.36030/2310-2837-2(101)-2021-39-46

КІБЕРГІГІЄНА ЯК СКЛАДОВА ФОРМУВАННЯ ЦИФРОВОЇ ДЕРЖАВИ

О. Ж. Скибун,
Адміністрація Державної служби спеціального зв'язку та захисту інформації України

У статті розглянуто роль кібергігієни як важливої складової у формуванні цифрової держави. Акцентовано увагу на тому, що реалізація програм та проєктів з інформатизації в рамках «Цифрової держави» та «Цифрової влади» створює запит на розвиток і вдосконалення цифрових компетентностей та навичок як у фахівців та спеціалістів, так і серед широких верств населення, адже цифровізація все далі проникає в усі сфери суспільства та суспільні відносини. Зазначено, що масова цифровізація широких верств населення породжує сплеск кіберзагроз, кіберінцидентів та кіберзлочинів, а це, у свою чергу, – запит на вироблення та дотримання певних умовностей та рекомендацій щодо зниження впливу кіберзагроз на подальшу цифровізацію, які повинні виконуватися практично підсвідомо (на рівні звичок). Вказане явище отримало назву – кібергігієна. Розглянуто рекомендації щодо дотримання кібергігієни, які необхідно поширювати (впроваджувати) на державному рівні через відповідні механізми, інструменти та методики поширення кібергігієни серед широких верств населення. Розглянуто доцільність створення фізичних «центрів кібердопомоги з надання безкоштовної допомоги населенню» та їх розміщенням у місцях «підвищення рівня діджиталізації», а саме: центрах надання адміністративних послуг, об'єднаних територіальних громадах, школах, бібліотеках. Наголошено на необхідності формування під час здобуття молодим поколінням освіти (дошкільної, середньої та вищої) кібергігієни.
Ключові слова: кібербезпека; кіберзагрози; кіберінциденти; цифровізація; інформатизація; віртуальний простір; «цифрова держава»; «цифрове суспільство»; кібергігієна.

CYBER HYGIENE AS A COMPONENT DIGITAL FORMATION

O. Zh. Skybun,
State Service of Special Communications and Information Protection of Ukraine

The article considers the role of cyberhygiene as an important component in the formation of the digital state. The implementation of informatization programs and projects within the «Digital State» and «Digital Power» creates a demand for the development and improvement of digital competencies and skills of professionals and professionals, as well as among the general population, as digitalization continues to penetrate alThus, it was noted that the mass digitalization of large sections of the population generates a surge of cyber threats, cyber incidents, and cybercrimes. This, in turn, creates a demand for the development and compliance with certain conventions and recommendations to reduce the impact of cyber threats on further digitization, the implementation of which must take place almost subconsciously (at the level of habits). This phenomenon is called – cyber hygiene. I spheres of society and public relations. To date, a significant level of cyber hygiene recommendations has been developed, which should be disseminated (implemented) at the state level through appropriate mechanisms, tools, and methods of disseminating cyber hygiene among the general population. To this end, it is proposed to consider the feasibility of creating physical «cyber help centers to provide free assistance to the population» and their placement in places of «increased digitalization», namely: administrative service centers, integrated communities, schools, libraries. As for the younger generation, cyber hygiene must be formed during education (preschool, secondary and higher).
Keywords: cybersecurity; cyber threats; cyber identities; digitalization; informatization; cyberspace; «digital state»; «digital society»; cyber hygiene.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Подальший розвиток науки і техніки разом з упровадженням технологій, обладнання в рамках цифрової та промислової революцій, використання їх широкими масами створюють передумови трансформацій суспільства в цілому, суспільних сфер і суспільних відносин. Вказане впливає на взаємовідносини на рівні людина-суспільство-влада.

Особливістю сучасного етапу цивілізаційного розвитку є те, що інформація набула ознаки товару та стратегічного ресурсу, а засоби виробництва формуються на інформаційно-цифровій складовій, де цифрова інформація стає суб'єктом товарно-виробничих відносин. При цьому економіка від виробництва поступово переходить до надання послуг та сервісів, де цифровий сектор починає переважати. Подальша цифровізація та інформатизація суспільно-політичних, суспільно-економічних, суспільно-гуманітарних відносин під час широкого впровадження програм і проєктів у рамках «цифрової держави» та «цифрового суспільства» суттєво впливають на людину, її життєві компетентності, навички, знання, внутрішній світ, поведінку, цінності тощо. В

умовах цифрових технологій, гаджетів, віртуального світу, соціальних мереж та глобальних комунікацій народилося нове цифрове покоління. На сьогодні нікого вже не дивує ситуація, коли мала дитина вправно справляється із різноманітними гаджетами, інколи ще не вміючи говорити. Також звичайною є ситуація, коли діти молодшого шкільного віку допомагають дідусям та бабусям орієнтуватися у світі цифрових технологій, смартфонів, планшетів, а також Інтернету речей та робототехніки (робот-пилосос, дистанційне ввімкнення побутових приладів тощо).

Додатковим поштовхом до підвищення рівня насичення різними комунікаційними пристроями стали події останніх років, пов'язані із поширенням коронавірусу та карантинними заходами боротьби з ним. Наприклад, аналітик Gartner Ранджит Атвал, коментуючи ситуацію на ринку програмованого кінцевого обладнання, зазначає, що «пандемія COVID-19 назавжди змінила те, як використовуються комп'ютерні пристрої співробітниками і споживачами», а «дистанційний режим роботи тепер змінився гібридним, домашнє навчання стало цифровим, а інтерактивні комп'ютерні ігри перемістилися в хмарне середовище» (Двойная мощность и новый ум), що створює передумови збільшення кількості типів і загальної кількості пристроїв, які необхідні для цього. Вказане підтверджується цифрами. Так, загальна кількість комп'ютерних пристроїв, включаючи ноутбуки, настільні ПК, планшети і мобільні телефони, які перебувають у використанні, в 2021 р. досягне 6,2 млрд штук, при цьому «тільки ноутбуків і планшетів у користувачів у цьому році додасться на 125 млн штук порівняно з 2020 роком» (Двойная мощность и новый ум). А враховуючи, що певна кількість настільних ПК, ноутбуків і планшетів перебуває у спільному використанні домогосподарств, сукупна кількість споживачів/користувачів послуг перевищує кількість одиниць техніки і може досягати понад 7 млрд осіб. Слід також зазначити, що, за даними Gartner, «у 2021 році кількість смартфонів у світі перевищить 4,3 млрд штук, а у 2022 наблизиться до 4,5 млрд штук», а (за даними Strategy Analytics) «продажі портативних ПК з підтримкою стільникового зв'язку в 2020 році вперше перевищили 10 млн штук», і на сьогодні «у світі використовуються понад 26 млн портативних комп'ютерів з вбудованими модулями 3G, 4G/LTE і 5G» і при цьому, як наголошують експерти, «смартфони передають особисті дані користувача в середньому кожні 4,5 хвилини» (Двойная мощность и новый ум).

Таким чином, можна стверджувати, що в умовах стрімкого зростання кількості програмованого кінцевого обладнання разом із розбудовою мережі міжнародних електронних комунікацій та глобальної мережі передачі даних стрімко зростає кількість користувачів. З одного боку, поширення цифрових технологій серед широких верств населення робить їх доступними, урівнюючи можливості віртуальних комунікацій серед найбагатших та найбідніших верств населення, а з другого виникає ситуація, коли поширення цифрових навичок та основ кіберзахисту і кібергігієни відстає від кількості програмованого кінцевого обладнання, що перебуває у населення. У зв'язку із цим «одними з найвразливіших місць віртуального світу є мобільний телефон із доступом до соціальних мереж, месенджерів, та десятків мобільних додатків часто невідомого походження, де люди з легкістю діляться приватною інформацією, яка, на перший погляд, не є критичною» (Безпека в Інтернеті). У зв'язку з цим виникає проблема підвищення рівня безпеки цифрових-, ІТ-, комп'ютерної, кібер- компетентностей до такого рівня, коли б кожний користувач переймався проблемами кіберзахисту і мав високий рівень особистої і колективної кібергігієни.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. Вплив кіберзагроз, кіберінцидентів на цифровий розвиток суспільства та роль кібергігієни у формуванні цифрової держави досліджували такі науковці, як: Є. Аушев, В. Богуш, Ю. Вишневський, О. Дашковська, В. Жора, Н. Ткачук, О. Юдін, С. Черняк та ін.

Проте, незважаючи на досить широкий спектр проведених досліджень, питання кібергігієни як складової формування цифрової держави досліджене не повною мірою і є частиною загальної проблеми, якій присвячена стаття.

Мета статті – дослідження розуміння важливості кібергігієни як складової формування цифрової держави в умовах підвищення рівня кіберзагроз та кіберінцидентів.

Виклад основного матеріалу. Подальший цивілізаційний розвиток суспільства (на базі інформаційного і навіть постінформаційного та постекономічного суспільств) формує нову цифрову глобальну людину, яка є досить мобільною, вільною, толерантною, добре розуміється на сучасних цифрових технологіях, гаджетах, робототехніці та Інтернеті речей. Звичайно, такій людині не потрібно пояснювати, що таке цифрове суспільство, цифрова держава, цифрова економіка. А тому у «цифровій реальності» почуває

себе впевнено лише цифрове покоління, діти, які народилися в період 2005–2010 рр. (так зване покоління Z) і пізніше. Усі попередні покоління досить повільно адаптуються та пристосовуються до цифрових реалій. Парадокс сучасності полягає в тому, що на сьогодні носіями «цифрового досвіду» виступають не попередні покоління (батьки, дідусі і бабусі), а діти і навіть внуки. Цифрові технології, міжнародні електронні комунікації та глобальна мережа передачі даних також повністю нівелювали такий важливий у традиційному світі поділ життєвого досвіду та життєвого світу на близький та далекий. Сьогодні в епоху глобалізації за допомогою цифрових технологій та програмованого кінцевого пристрою (ПКП) перейняти та/або передати досвід, знання, навички можна із однієї точки земної кулі в іншу практично миттєво. Крім того, наявність сучасного ПКП залежить не від країни, національності, віросповідання користувача, а від наявності електронних комунікацій та глобальної мережі передачі даних, які постійно розширюються та охоплюють все більше території і населення. Ось чому ПКП можна побачити як у користувача із високорозвиненої країни, так і у корінних жителів Амазонії, Африки та ін., тобто сучасні технології роблять світ менш сегрегованим, хоча на загальний стан цифровізації впливає цивілізаційний розвиток, державний лад і політичний устрій, рівень освіти, освіченості та «цивілізованості». Цим і характеризується різна швидкісність процесів переходу суспільства окремих країн на новий рівень цивілізаційного розвитку суспільства, який уже набуває ознак постінформаційного та постекономічного. Але незважаючи на це рівень цифровізації та інформатизації суспільства щорічно тільки підвищується, і ця тенденція лише зростає. Це пов'язано із масовим переходом економіки на нові етапи, формування яких відбувається під впливом цифрової та четвертої промислової революцій.

На сьогодні цифрові технології (поєднання традиційних сфер із кіберсферою, особливо в медичній сфері), робототехніка, системи штучного інтелекту та проєкти Smart City, суперкомп'ютери та робота із значними масивами даних (наукова сфера, прогнозування, генетика, системи управління) стають буденними і звичними для пересічного громадянина переважної більшості країн світу (через широке впровадження програм та проєктів з інформатизації). Але поряд із перевагами, пов'язаними з глобальними електронними комунікаціями, цифровими технологіями, цифровізацією та інформатизацією всіх сфер суспільства та суспільних процесів, з'являються нові загрози та виклики – кіберзагрози (кібершахрайство, кібершпигунство, кіберзлочини тощо). Додатковим і навіть несподіваним каталізатором сплеску вказаних вище кіберзлочинів стали заходи, які вживалися впродовж останніх двох років проти поширення світом пандемії коронавірусу (COVID-19), а саме масовий перехід від офлайн- до онлайн-комунікацій на всіх рівнях взаємовідносин між громадянином-суспільством-владою. Завдяки карантинним заходам та фізичному закриттю закладів освіти, медицини, культури, спорту, сфери надання послуг (передусім побутових, банківських та адміністративних) значно підвищився рівень онлайн-комунікацій.

Іншим важливим аспектом є формування та впровадження державної політики у сфері цифровізації та інформатизації суспільства і влади в частині збільшення обсягів надання адміністративних послуг та сервісів до доступу до інформації в режимі онлайн. Основними їх напрямами є проєкти із розгортання центрів надання адміністративних послуг (ЦНАП) (https://decentralization.gov.ua/cnap, https://guide.diia.gov.ua/asc/), упровадження електронних адміністративних послуг (Урядовий портал. Єдиний вебпортал органів виконавчої влади (https://www.kmu.gov.ua/servicesfilter), єдиний державний портал адміністративних послуг (https://my.gov.ua/)) та створення сервісної інтернет-платформи, на якій запроваджено та функціонує «Дія: державні послуги онлайн» (https://diia.gov.ua/). Також масово створюються портали надання послуг онлайн підприємствами сфер житлово-комунального господарства (ЖКГ), енергетики, постачання тепла та води, а також центри комунального сервісу (наприклад центр комунального сервісу в м. Києві (https://cks.com.ua/cabinet/objects/), централізоване водопостачання та водовідведення (ПАТ АК «Київводоканал») (https://my.vodokanal.kiev.ua/), постачання електроенергії (ТОВ «Київські енергетичні послуги» (https://www.kyiv.yasno.com.ua/), постачання побутового газу (https://cabinet-energy.kyivgaz.ua/login, https://104.ua/ua/) тощо). Передусім споживачі послуг/громадяни стикнулися із необхідністю заміни застарілих гаджетів на нові ПКП, певну адаптацію та освоєння користування, що потребує підвищення рівня цифрової грамотності (комп'ютерної, ІТ тощо), цифрових компетентностей та навичок для можливості комунікації в режимі онлайн. Під час заміни застарілих гаджетів на нові ПКП, крім фінансової спроможності окремих груп населення до таких дій, виникає потреба у завантаженні необхідного

програмного забезпечення та навчання користування ним. Насамперед це стосується самотніх літніх людей та людей, яким нікому допомогти це зробити на особистісному рівні комунікацій. Але, незважаючи на це, виявилося, що за останні два роки кількість звернень онлайн суттєво зросла, при цьому середньостатистичне домогосподарство (власник) для комунікації із постачальниками послуг повинен створити відповідні особисті кабінети і надати певні персональні дані. Крім того, оплата за отримані послуги також здійснюється за допомогою мобільного банкінгу, тобто ПКП фактично кожного дорослого громадянина став носієм та комунікатором певного обсягу даних, ресурсів та інструментів для вчинення різних дій в режимі онлайн, що, у свою чергу, підвищило увагу шахраїв. У зв'язку із цим «кількість інтернет-шахрайств, фактів втручання в особистий простір, поширення неправдивих відомостей тощо нині набуває рис епідемії», коли нехтуються (свідомо чи через незнання) так звані «базові правила цифрової безпеки при роботі у світовій мережі та використанні різноманітних сервісів, що їх пропонують сучасні технології» (Кібергігієна). Це стосується рівня фізичних осіб та приватних комунікацій, перебування в соціальних мережах, послуг ЖКГ, банківських послуг (е-банкінг) тощо. Разом зі збільшенням кількості адміністративних електронних послуг та послуг в додатку «Дія» збільшується обсяг комунікації між громадянами і державою та відбувається обмін інформацією, персональними даними, паролями, що також викликає інтерес з боку шахраїв, адже збільшення обсягів звернень збільшує відсоток жертв від шахрайських дій. Важливим є те, що приватні і державні інформаційно-телекомунікаційні системи та обладнання забезпечуються комплексними системами захисту, супроводжуються відповідними підрозділами і мають певний рівень стійкості перед кіберзагрозами. Як зазначає В. Жора, «… захистити реєстри – це частина державної політики, і це частина наших обов'язків як служби, яка формує державну політику у сфері захисту інформації. Це захист самого додатка, і тут, очевидно, теж ведеться величезна робота. Але ми не можемо гарантувати безпеку кінцевого пристрою, крім рекомендацій для його власника як убезпечитися» (Жора). Ось чому ПКМ споживачів/громадян стають досить легкою мішенню для кібершахраїв. Ураховуючи кількість (масовість) ПКМ, що перебувають у приватному користуванні, можна констатувати високий рівень кіберзагроз для національної безпеки під час упровадження проєктів у рамках «Цифрової держави» та «Цифрового суспільства». При цьому необхідно пам'ятати, що найбільш ефективним є не боротьба з наслідками, а вживання превентивних заходів щодо мінімізації впливу кіберзлочинів та кібершахрайства.

Як відомо, найненадійнішим елементом у системі взаємодії людина-машина, людина-машина-людина є людина, а тому слід починати з неї. Ось чому наступною після цифрових компетентностей та навичок є кібергігієна. Так, кібергігієна – це, передусім, самооцінка своїх ризиків, коли розуміння дотримання кібергігієни закріплюється на підсвідомому рівні і сприймається «так само, як мити руки перед їжею» (Безпека в Інтернеті), адже дотримання кібергігієни сьогодні стає основним питанням безпеки людини (не тільки в кіберпросторі, а й на фізичному рівні). Спеціалісти ESET під «кібергігієною» розуміють «заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації» (Основні правила захисту даних). У свою чергу, фахівці ITech розглядають кібергігієну як термін, «який використовується для захисних процедур вашої особистої та фінансової інформації під час використання комп'ютера чи мобільного пристрою», коли «хороша кібергігієна означає дотримання розумних щоденних практик щодо здоров'я та безпеки вашої інформації в Інтернеті» і серед іншого включає регулярне оновлення програмного забезпечення браузера, встановлення та підтримку програмного забезпечення для захисту, вибір надійних паролів, заборону ділитися паролями, а також уникнення загальнодоступного Wi-Fi для онлайн-банкінгу та інших фінансових операцій», що, зрештою, зменшить вірогідність контакту із кібершахраями та кіберзлодіями (Кібергігієна... Що це?). Так, «для забезпечення захисту ваших персональних даних під час роботи в мережі «Інтернет» спеціалісти ESET рекомендують дотримуватися основних правил кібергігієни», а саме: «перевірка безпеки активних акаунтів, аналіз програм, регулярне оновлення, надійний пароль, додатковий рівень захисту, регулярне резервне копіювання, надійний захист» (Основні правила захисту даних). Фахівці ITech пропонують 10 порад, які не дадуть змоги підхопити вірус в інтернеті: «остерігайтеся підроблених кнопок завантаження, використовуйте безпечний браузер, не розмовляйте з телефонними шахраями, ігноруйте оголошення, які спливають, на тему безпеки, уникайте публічних торент-сайтів, видаліть медіафайли, що вимагають підроблених кодексів,

не відкривайте вкладення електронної пошти, отримані від невідомих, не використовуйте обліковий запис адміністратора свого ПК, скануйте всі нові файли та диски» (Десять порад). Наведені рекомендації є зрозумілими для виконання середньостатистичним користувачем ПКП. Ось чому «важливо дотримуватись правил зі своїми гаджетами», зокрема таких «Не підключатись до публічного WiFi. Використовуйте краще мобільний інтернет. Якщо дуже треба підключитись, то робіть це із використанням VPN (не безкоштовного); не переходьте за посиланнями, які вам невідомо чому присилають, навіть якщо це ваші знайомі зі знайомих акаунтів. Часто зловмиснику потрібно від вас тільки один клік за посиланням, щоб отримати доступ до вашого профілю; не додавайте незнайомих людей у друзі у фейсбук, бо вони можуть відправляти інформацію вашим колегам вже у статусі вашого друга; змінюйте паролі кожні 2–3 місяці, використовуйте різні складні паролі, які важко вирахувати, та двофакторну аутентифікацію не через СМС, а через додаток; завжди встановлюйте автоматичні оновлення версій програмного забезпечення. Якщо вже вийшло оновлення, цілком можливо, що у старій версії є вразливості; робіть регулярні бекапи важливої інформації, сегментуйте дані; перевіряйте, щоб сайт, яким ви користуєтесь, був https, а не http; хоча б раз на кілька років ходіть на тренінги з кібербезпеки. Запросіть туди своїх дітей-підлітків та колег по роботі» (Безпека в Інтернеті).

Перелічені вище рекомендації необхідно виконувати як на роботі, так і вдома. Підвищення рівня цифровізації інформаційних процесів (електронний документообіг) в органах державної влади всіх рівнів, а також широке використання глобальної мережі передачі даних сприяли збільшенню кількості кіберінцидентів на робочому місці. Крім того, подальше впровадження програм та проєктів з інформації в рамках «Цифрової держави» та «Цифрового суспільства» постійно розширює перелік адміністративних послуг, реєстрів та баз даних, де концентруються великі масиви даних, у тому числі і персональних даних громадян. У зв'язку із цим відсоток кіберінцидентів також зростає, передусім через «людський фактор», коли людина не дотримується вимог кібергігієни. Це призводить до таких наслідків, як: несанкціонований доступ до баз даних; копіювання та передача через незахищений канал мережі «Інтернет» документальних матеріалів, що містять службову інформацію; використання особистих ПКП у складі виробничих автоматизованих систем (USB-флеш накопичувані, зовнішні жорсткі диски); підключення до комп'ютерних систем технічних засобів із модулями передачі даних (Wi Fi, Bluetooth, GSM тощо), призначених для створення каналів зв'язку з іншими електронними пристроями, а також приєднання до телекомунікаційних мереж загального користування; слабка захищеність ПКП через застарілі версії антивірусного програмного забезпечення. Усунення перелічених вище дій сприятиме підвищенню рівня кібербезпеки (зменшить кількість кіберінцидентів через «людський фактор»). Як зазначає В. Жора, важливим завданням, яке потребує негайного вирішення, є «кібербезпека в кожен дім. Кожен громадянин може розраховувати на власну безпеку в кіберпросторі. Ми не можемо фізично дійти до кожного громадянина, але кожен громадянин може усвідомити правила поведінки в кіберпросторі. На своєму кінцевому пристрої людина сама відповідальна за захист, а в умовах карантину, коли вона працює вдома, користується корпоративною поштою, підключається до конференцій, обмінюється файлами, вона має вразливу точку» (Жора).

На сьогодні вживаються різні заходи стосовно формування дотримання умов кібергігієни якомога ширшої аудиторії, передусім не пов'язаної професійно із питаннями кіберзахисту та кібербезпеки. Так, у січні 2021 р. «Міністерство цифрової трансформації України та Координатор проєктів ОБСЄ в Україні презентували новий освітній серіал «Основи кібергігієни», успішна демонстрація якого дасть змогу «знати й застосовувати правила кібергігієни на роботі й у повсякденні; розуміти суть соціальної інженерії та психології впливу; безпечно користуватися браузером та загалом мережами Wi-Fi; розмежовувати використання особистої та службової поштових скриньок; розбиратися у використанні програмного забезпечення; вміти відповідально поширювати інформацію в соціальних мережах; опанувати правила безпечної роботи з мобільними пристроями; ознайомитися з роллю фізичної безпеки в кіберзахисті організації; розбиратися у видах маніпуляцій з інформацією у кіберсфері» (Мінцифри навчить).

Водночас «Представники Фонду цивільних досліджень та розвитку CRDF Global (США) запропонували впровадити в КПІ розроблений його фахівцями у співпраці з експертами з кібербезпеки та за підтримки Офісу з координації допомоги в Європі та Євразії Державного департаменту США безкоштовний онлайн-курс з кібергігієни «Базові правила безпеки у цифровому середовищі» (Кібергігієна). Також в Україні «за

фінансової підтримки урядів Великої Британії та Німеччини» реалізується проєкт «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки» (Мінцифри навчить).

Разом з тим у рамках Нової Української школи запроваджено нову ключову компетентність, яка повинна розвиватися у школі, а саме «інформаційно-цифрову компетентність», яка «… передбачає впевнене, а водночас критичне застосування інформаційно-комунікаційних технологій (ІКТ) для створення, пошуку, обробки інформації та обміну нею на роботі, в публічному просторі та приватному спілкуванні», інформаційну й медіаграмотність, знання основ програмування, алгоритмічне мислення, роботу з базами даних, навички безпеки в інтернеті та кібербезпеці, розуміння етики роботи з інформацією (авторське право, інтелектуальна власність тощо)» (Нова Українська школа, 2016).

Указане знайшло відображення в Державному стандарті базової середньої освіти, де зазначається, що «інформаційно-комунікаційна компетентність передбачає впевнене, критичне і відповідальне використання цифрових технологій для власного розвитку і спілкування; здатність безпечно застосовувати інформаційно-комунікаційні засоби в навчанні та інших життєвих ситуаціях, дотримуючись принципів академічної доброчесності» (Державний стандарт, 2020), а тому «цифрова компетентність» – це «динамічна комбінація знань, умінь, навичок, способів мислення, поглядів, інших особистих якостей у сфері інформаційно-комунікаційних та цифрових технологій, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність із використанням таких технологій» (Про схвалення Концепції, 2021).

У цілому можна говорити про потужний пул освітніх програм, які охоплюють практично всю активну аудиторію кіберпростору. Насамперед регулярні заходи із підвищення рівня цифрової компетентності повинні стосуватися тієї частини державних службовців, військових та найманих працівників, які взаємодіють, супроводжують, наповнюють державні інформаційні ресурси, а також забезпечують функціонування інформаційно-телекомунікаційних систем, які виступають базисом цифрової країни.

На сьогодні Міністерство цифрової трансформації України запустило національний проєкт «Дія. Цифрова освіта», на базі якого пропонується проводити навчання за різними напрямами, це насамперед, цифрова освіта.

Наприклад, Українською школою урядування здійснюється підвищення кваліфікації за загальною короткостроковою програмою «Основи кібергігієни», навчання за якою відбувається дистанційно на навчальній платформі за таким посиланням «Дія. Цифрова освіта» (https://osvita.diia.gov.ua/courses/cyber-hygiene) або «Спільнота практик: сталий розвиток» (https://udl.despro.org.ua/enrol/index.php?id=149).

Отже, активна частина суспільства, яка навчається та працює, має більше переваг порівняно із тією частиною суспільства (пенсіонери, а також учасники кібервзаємовідносин, які нечасто користуються державними інформаційними ресурсами), що за родом своєї діяльності не стикається із кіберпростором, а є лише приватним споживачем послуг та користувачем електронних комунікацій і споживачем ресурсів віртуального простору (соціальні мережі, соціальні медіа, е-розваги, е-торгівля, е-банкінг тощо). У зв'язку із цим було б доцільно більш активно і широко проводити інформаційну кампанію через засоби масової комунікації, які орієнтовані на вказану цільову аудиторію, а також запропонувати відповідні методики та інструменти навчання.

Так, у рамках Концепції розвитку цифрових компетентностей передбачені такі шляхи «підвищення рівня обізнаності громадян щодо небезпек в інтернеті»: «створення соціальних ініціатив, спрямованих на підвищення рівня цифрових навичок та цифрових компетентностей для представників різних цільових груп населення» та «запровадження програм, спрямованих на підвищення рівня обізнаності дітей та підлітків, цифрових компетентностей батьків та педагогічних працівників щодо небезпек дитини у цифровому середовищі, формування культури нетерпимого ставлення до порушення прав, свобод, безпеки дитини в цифровому середовищі» (Про схвалення Концепції, 2021).

Що стосується практичної сторони, то на сьогодні створено безліч інструментів «фізичної комунікації». Як приклад можна розглянути доцільність створення «центрів кібердопомоги з надання безкоштовної допомоги населенню» і розміщувати їх у місцях надання адміністративних та освітніх послуг, а саме: ЦНАПах, ОТГ, школах, бібліотеках (у тих громадських установах, які є у певному населеному пункті).

Крім освітніх та інформаційно-роз'яснювальних послуг, слід передбачити можливість встановлення (на вимогу) антивірусних програм

на ПКП, видалення вірусів та уражених програм, а також установлення необхідного програмного продукту на ПКП, для того щоб можна було використовувати його як інструмент комунікації з бізнесом, владою, суспільством у рамках «Цифрової держави» та «Цифрової країни».

Висновки та перспективи подальших досліджень. Підсумовуючи дослідження кібергігієни як складового елемента формування цифрової держави, можна констатувати ось що. Подальший цивілізаційний розвиток суспільства відбувається під впливом цифровізації та інформатизації всіх сфер суспільства, соціальних відносин, людського буття. Науково-технічний прогрес (цифрова і четверта промислова революції) формують новий тип людини, суспільства та взаємовідносин на рівні людина-суспільство-влада. Поступово віртуальна реальність (кіберпростір) починає домінувати над фізичним реальним світом, змінюючи світ навколо людини. Серйозний вплив на ці процеси справляється під час реалізації програм та проєктів з інформатизації в рамках «Цифрової держави» та «Цифрової влади». Вказане створює запит на розвиток та вдосконалення цифрових компетентностей та навичок. Масова цифровізація широких верств населення призвела до сплеску кіберзагроз, кіберінцидентів та кіберзлочинів, які зростають разом із цифровізацією. Це спричинило запит на вироблення й дотримання певних умовностей та рекомендацій щодо зменшення впливу кіберзагроз на подальшу цифровізацію, що отримало назву кібергігієни. На сьогодні напрацьовано значний обсяг рекомендацій щодо дотримання кібергігієни на рівні як простих споживачів цифрових послуг, так і тих, хто є відповідальним за ведення, наповнення, збереження та обробку персональних даних, баз даних та інформаційних ресурсів (державного, приватного та бізнес-рівнів).

Для підвищення рівня дотримання кібергігієни необхідно розроблення та впровадження (на державному рівні) відповідних механізмів, інструментів та методик поширення кібергігієни серед усіх верств населення. Особливо слід звертати увагу на верстви населення, які не є активними суб'єктами цифрового суспільства, а використовують цифрові технології з огляду на потреби сьогодення. Водночас необхідно забезпечити надання кібердопомоги на всій території країни. Для цього пропонується розглянути доцільність створення «центрів кібердопомоги з надання безкоштовної допомоги населенню» із розміщенням їх у місцях «підвищеного рівня діджиталізації», а саме: ЦНАПах, ОТГ, школах, бібліотеках (у тих громадських установах, які є у певному населеному пункті). Що стосується молодого покоління, то кібергігієну необхідно формувати під час здобуття освіти (дошкільної, середньої та вищої).

Подальше підвищення рівня цифровізації держави та суспільства створює передумови до збільшення кількості кіберзлочинів, кіберзагроз та кіберінцидентів, що передбачає підвищену відповідальність суспільства за дотримання рекомендацій та правил з кібергігієни, а це потребує додаткових розвідок.

Список використаних джерел

Безпека в Інтернеті: найпростіші правила захисту даних. URL: https://www.bbc.com/ukrainian/blogs-51444737 (дата звернення: 01.06.2021).

Двойная мощность и новый ум. Каким будет последнее поколение смартфонов. URL: https://www.dsnews.ua/future/dvoynaya-moshchnost-i-novyy-um-kakim-budet-sleduyushchee-poslednee-pokolenie-smartfonov-16052021-425130 (дата звернення: 30.05.2021).

Державний стандарт базової середньої освіти : Постанова Каб. Міністрів України від 30.09.2020 № 898. *Офіц. вісн. України.* 2020. № 81. Ст. 2615.

Десять порад, які не дозволять підхопити вірус в Інтернеті. URL: https://itech.co.ua/novyny/10-porad-iaki-ne-dozvoliat-pidkhopyty-virus-v-interneti/ (дата звернення: 01.06.2021).

Жора В. Може, у кіберНАТО ми будемо швидше, ніж у реальному. URL: https://www.ukrinform.ua/rubric-technology/3249583-viktor-zora-zastupnik-golovi-derzavnoi-sluzbi-specialnogo-zvazku-ta-zahistu-informacii-ukraini.html90щ (дата звернення: 29.05.2021).

References

Bezpeka v Interneti: najprostishi pravy`la zaxy`stu dany`x. Retrieved from: https://www.bbc.com/ukrainian/blogs-51444737 (accesed: 01.06.2021).

Dvoynaya moschnost i novyiy um. Kakim budet poslednee pokolenie smartfonov. Retrieved from: https://www.dsnews.ua/future/dvoynaya-moshchnost-i-novyy-um-kakim-budet-sleduyushchee-poslednee-pokolenie-smartfonov-16052021-425130 (accesed: 30.05.2021).

Derzhavny`j standart bazovoyi seredn`oyi osvity` : Postanova Kabinetu Ministriv Ukrayiny` vid 30 veresnya 2020 # 898. *Oficijny`j visny`k Ukrayiny`*. # 81. St. 2615 [in Ukrainian].

Desyat` porad, yaki ne dozvolyat` pidxopy`ty` virus v Interneti. Retrieved from: https: https://itech.co.ua/novyny/10-porad-iaki-ne-dozvoliat-pidkhopyty-virus-v-interneti/ (accesed: 01.06.2021).

Zhora, V. Mozhe, u kiberNATO my` budemo shvy`dshe, nizh u real`nomu. Retrieved from: https://www.ukrinform.ua/rubric-technology/3249583-viktor-zora-zastupnik-golovi-derzavnoi-sluzbi-specialnogo-zvazku-ta-zahistu-informacii-ukraini.html90щ (accesed: 29.05.2021).

Кібергігієна – це важливо! URL: https://kpi.ua/2020-10-28 (дата звернення: 31.05.2021).

Кібергігієна … Що це? І 5 речей, які слід знати про це. URL: https://itech.co.ua/novyny/kiberhihiiena-shcho-tse-i-5-rechej-iaki-slid-znaty-pro-tse/ (дата звернення: 01.06.2021).

Мінцифри навчить держслужбовців основ кібергігієни. URL: https://www.kmu.gov.ua/news/mincifra-navchit-derzhsluzhbovciv-osnov-kibergigiyeni (дата звернення: 01.06.2021).

Нова українська школа. Концептуальні засади реформування середньої школи. МОН 27/10/2016. 40 с. URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/nova-ukrainska-shkola-compressed.pdf (дата звернення: 02.06.2021).

Основні правила захисту даних – кібергігієна для активного Інтернет-користувача. URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya (дата звернення: 01.06.2021).

Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : Розпорядження Каб. Міністрів України від 03.03.2021 № 167-р. *Уряд. кур'єр.* 2021. 16 берез. № 50.

Стратегія кібербезпеки України (2021–2025 роки) : проєкт. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 31.05.2021).

Юдін О. К., Богуш В. М. Інформаційна безпека держави. Харків : Консум, 2004. 508 с.

Kibergigiyena – ce vazhly`vo! Retrieved from: https://kpi.ua/2020-10-28 (accesed: 31.05.2021).

Kibergigiyena … Shho ce? I 5 rechej, yaki slid znaty` pro ce (2020). Retrieved from: https://itech.co.ua/novyny/kiberhihiiena-shcho-tse-i-5-rechej-iaki-slid-znaty-pro-tse/ (accesed: 01.06.2021).

Mincy`fry` navchy`t` derzhsluzhbovciv osnov kibergigiyeny`. Retrieved from: https://www.kmu.gov.ua/news/mincifra-navchit-derzhsluzhbovciv-osnov-kibergigiyeni. (accesed: 01.06.2021).

Nova ukrayins`ka shkola. Konceptual`ni zasady` reformuvannya seredn`oyi shkoly`. (2016). MON 27/10/2016. 40 p. Retrieved from: https://mon.gov.ua/storage/app/media/zagalna%20serednya/nova-ukrainska-shkola-compressed.pdf (accesed: 02.06.2021).

Osnovni pravy`la zaxy`stu dany`x – kibergigiyena dlya akty`vnogo Internet-kory`stuvacha. Retrieved from: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya (accesed: 01.06.2021).

Pro sxvalennya Koncepciyi rozvy`tku cy`frovy`x kompetentnostej ta zatverdzhennya planu zaxodiv z yiyi realizaciyi (2021) : Rozporyadzhennya Kabinetu Ministriv Ukrayiny` vid 3 bereznya 2021 № 167-r. Uryadovy`j kur'yer vid 16.03.2021 # 50 [in Ukrainian].

Strategiya kiberbezpeky` Ukrayiny` (2021–2025 roky) : proekt. Retrieved from: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (accesed: 31.05.2021).

Yudin, O. K., Bogush, V. M. Informacijna bezpeka derzhavy`. Xarkiv : Konsum, 2004. 508 s. [in Ukrainian].

Скибун Олександр Жоржович,
кандидат наук з державного управління, Адміністрація Державної служби спеціального зв'язку та захисту інформації,
03110, Україна, м. Київ, вул. Солом'янська, 13

Цитування: Скибун О. Ж. Кібергігієна як складова формування цифрової держави. *Вісн. НАДУ. Серія «Державне управління»*. 2021. № 2 (101). С. 39–46.

Стаття надійшла: 18.05.2021

Схвалено до друку: 24.05.2021

Skybun, Oleksandr Zh.,
Candidate of Science in Public Administration,
State Service of Special Communications and Information Protection of Ukraine,
13, Solomianska St., Kyiv, 03110, Ukraine
E-mail: skybun@i.ua
http://orcid.org/0000-0001-6084-5222

Citation: Skybun, O. Zh. (2021). Kiberhihiiena yak skladova formuvannia tsyfrovoi derzhavy [Cyber hygiene as a component digital formation]. *Bulletin of the NAPA. Series «Public Administration».* Is. 2 (101). P. 39–46 [in Ukrainian].

Article arrived: 18.05.2021

Accepted: 24.05.2021